

ЗАТВЕРДЖЕНО
ЄААД.468244.185-ЛУ

Інв. № орг.	
Підп. та дата	
Взам. інв. №	
Інв. № дубл	
Підп. та дата	

Центр сертифікації ключів ринку електричної енергії

Комплекс засобів синхронізації часу

Загальний опис системи

ЄААД.468244.185.ПД.03

2014 р.

ЗМІСТ

1 ПРИЗНАЧЕННЯ КОМПЛЕКСУ	4
2 ОПИС КОМПЛЕКСУ	5
2.1 Структура комплексу та призначення технічних засобів.....	5
2.2 Характеристики GPS-приймача	5
2.3 Опис функціонування комплексу	5
2.4 Умови застосування	6
3 СКЛАД ТЕХНІЧНОГО ОБЛАДНАННЯ, ЩО ЗАСТОСОВУЄТЬСЯ У ПРОЦЕСІ СИНХРОНІЗАЦІЇ, ЙОГО ЗАГАЛЬНИЙ ОПИС	7
3.1 Структура комплексу засобів синхронізації часу.....	7
3.2 Перелік технічних та програмних засобів синхронізації часу	7
4 ПОРЯДОК СИНХРОНІЗАЦІЇ	9
4.1 Порядок синхронізації	9
4.2 Методика синхронізації часу в штатних ситуаціях.....	9
4.3 Методика синхронізації часу в аварійних ситуаціях	9
4.4 Операційний контроль.....	9
ДОДАТОК 1. КОНФІГУРАЦІЯ NTP-СЕРВЕРА ЦЕНТРУ СЕРТИФІКАЦІЇ КЛЮЧІВ.....	10

ПЕРЕЛІК СКОРОЧЕНЬ

БД	- База даних
ВОЛЗ	- Волоконно-оптичні лінії зв'язку
ДБЖ	- Джерело безперебійного живлення
ЕОМ	- Електронно-обчислювальна машина
ЕОТ	- Електронно-обчислювальна техніка
ЕЦП	- Електронний цифровий підпис
ЄСПД	- Єдина система програмної документації
ЗТМ	- Зовнішні телекомунікаційні мережі
ІТС	- Інформаційно-телекомунікаційна система
КЗЗ	- Комплекс засобів захисту
КЗІ	- Криптографічний захист інформації
КТЗ	- Комплекс технічних засобів
КСЗІ	- Комплексна система захисту інформації
ЛОМ	- Локальна обчислювальна мережа
МЕ	- Міжмережний екран
НКІ	- Носій ключової інформації
НМС	- Накопичувач на магнітній стрічці
ОС	- Операційна система
ПЕОМ	- Персональна ЕОМ
ПЗ	- Програмне забезпечення
ПЗП	- Постійний запам'ятовуючий пристрій
ПРД	- Правила розмежування доступу
ПТК	- Програмно-технічний комплекс
РС	- Робоча станція
СУБД	- Система управління базами даних
ТЗІ	- Технічний захист інформації
ЦСК	- Центр сертифікації ключів
СМР	- Control Messages Protocol (протокол управляючих повідомлень)
GPS	- Global Positioning System (глобальна система позиціонування)
HTTP	- Hyper Text Transfer Protocol
LDAP	- Lightweight Directory Access Protocol (протокол доступу до каталогу)
MTA	- Mail Transfer Agent (модуль передачі електронних поштових повідомлень)
OCSP	- Online Certificate Status Protocol (протокол визначення статусу сертифіката)
TSP	- Time-Stamp Protocol (протокол отримання позначок часу)

1 ПРИЗНАЧЕННЯ КОМПЛЕКСУ

Комплекс призначений для забезпечення синхронізації часу у технічних засобах програмно-технічного комплексу ЦСК.

Комплекс забезпечує:

- отримання часу з 4-12 супутників GPS;
- отримання точного часу з NTP-серверів Центрального засвідчувального органа;
- синхронізацію системного часу на технічних засобах ЛОМ програмно-технічного комплексу ЦСК.

2 ОПИС КОМПЛЕКСУ

2.1 Структура комплексу та призначення технічних засобів

До складу комплексу входять такі програмні та технічні засоби:

- GPS-приймач;
- програмний комплекс сервера моніторингу та синхронізації часу (далі - ПК сервера синхронізації);
- програмний комплекс клієнта синхронізації часу (далі - ПК клієнта синхронізації часу).

Функціональна структура комплексу ЦСК наведена на рис. 2.1.

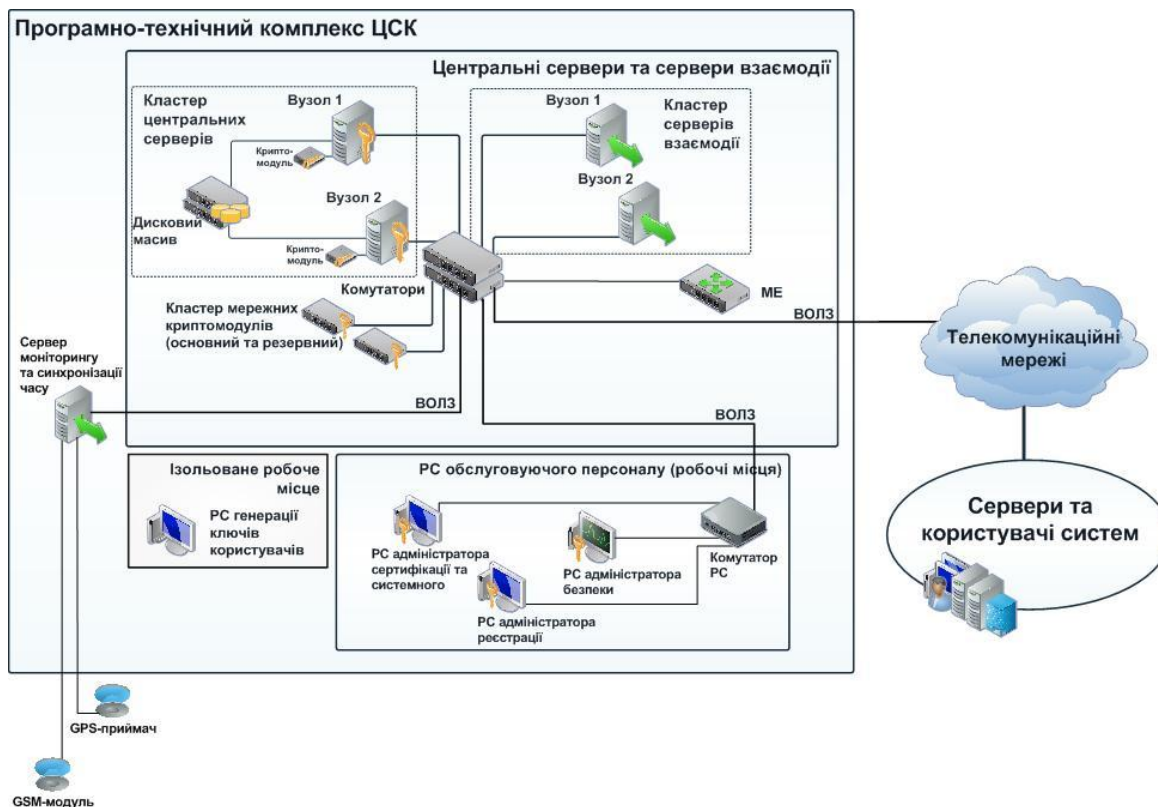


Рисунок 2.1- Функціональна структура комплексу ЦСК

2.2 Характеристики GPS-приймача

В якості GPS-приймача на PC чи сервері синхронізації часу використовується 14-ти каналний GPS(ГЛОНАСС)-приймач NovaTel SMART V-1 ANTENNA на основі OEM-карти OEM-V1G та антени GPS-521, або EPS Agro-DM-1Hz.

Даний GPS-приймач конструктивно виконаний як GPS-приймач та антена в одному корпусі (корпус є закритим та захищеним у відповідності до стандарту MIL-STD 810E).

Параметри GPS-приймача:

- 14 каналів L1 GPS;
- 2 канали L1SBAS;
- широкий діапазон вхідного живлення від 9 до 36 В постійного току, захист від перенавантаження SAE J1455;
- вихід 1 PPS (імпульс в секунду), синхронізований зі шкалою GPS з точністю ± 20 нс.

GPS-приймач може отримувати інформацію від 4-14 супутників. Значення точного часу отримуються у всесвітній шкалі UTC із точністю 1с.

2.3 Опис функціонування комплексу

Сервер взаємодії ЦСК виступає в ролі клієнта NTP-сервера ЦЗО або в ролі клієнта резервних NTP-серверів, синхронізованих з державним еталоном одиниць часу і частоти, та є основним NTP-сервером для

ЦСК. В разі виходу за ладу NTP-сервера ЦЗО, резервних NTP-серверів або пошкодження каналу зв'язку з ЦЗО в якості NTP-сервера виступає сервер моніторингу та синхронізації часу, що отримує час від GPS-приймача.

Основним джерелом часу для засобів ЦСК є NTP-сервер сервера взаємодії ЦСК (далі NTP-сервер ЦСК).

Всі PC та сервери підключаються до NTP-сервера ЦСК та синхронізують системний годинник у відповідності до значення часу, що отримується від нього.

Штатний програмний NTP-сервер ОС сервера взаємодії ЦСК реалізований у вигляді демону (у ОС Linux - NTP daemon program). NTP-сервер настраюється за допомогою файлу конфігурації ntp.conf. Параметри файлу конфігурації що рекомендуються до встановлення наведені у дод. 2.

Штатні програмні NTP-клієнти ОС налагоджуються на всіх PC та серверах ЛОМ на отримання часу від NTP-сервера ЦСК за протоколом NTP. NTP-клієнти здійснюють підключення до NTP-сервера та отримують значення точного часу і виконують встановлення власного системного часу (системного годинника).

NTP-клієнти реалізовані у вигляді системних служб (у ОС Microsoft Windows) або демонів (у ОС Linux). Запуск NTP-клієнтів виконується автоматично ОС при її завантаженні.

NTP-сервер ЦСК здійснює обробку запитів від NTP-клієнтів PC та серверів ЛОМ та передачу їм значення точного часу для синхронізації власних системних годинників. Підключення NTP-клієнтів до NTP-сервера здійснюється за протоколом NTP (UDP/IP, номер UDP-порта - 123).

Сервер моніторингу та синхронізації часу ЦСК є резервним NTP-сервером для сервера взаємодії ЦСК. До складу функціонального ПЗ сервера моніторингу та синхронізації часу входить ПК сервера синхронізації часу та штатний програмний NTP-сервер ОС.

До сервера моніторингу та синхронізації часу ЦСК підключається GPS(ГЛОНАСС)-приймач. У ПК сервера синхронізації часу встановлюються такі параметри щодо роботи з приймачем:

- COM-порт підключення GPS-приймача;
- інтервал отримання значення часу з GPS-приймача у секундах;
- ознака отримання значення часу у разі відсутності видимих супутників.

Ознака отримання значення часу у разі відсутності видимих супутників - вказує на необхідність використання власного таймеру GPS - приймача в разі відсутності видимих супутників.

ПК сервера синхронізації часу виконує отримання значення часу з супутників через GPS(ГЛОНАСС)-приймач та виконує синхронізацію (встановлення) часу власного системного годинника PC чи сервер синхронізації часу.

2.4 Умови застосування

2.4.1 Загальносистемне програмне забезпечення

Вимоги до загальносистемного програмного забезпечення, в середовищі яких функціонують складові частини комплексу наведені у таблиці 2.1.

Таблиця 2.1

Складова частина комплексу	Вимоги до загальносистемного програмного забезпечення
Програмний компонент сервера синхронізації часу	ОС Microsoft Windows 7/8.1/2008 Server/2012 Server, Linux/Unix
Програмні компоненти клієнта синхронізації часу	ОС Microsoft Windows 7/8.1/2008 Server/2012 Server, Linux/Unix

2.4.2 Спеціальне програмне забезпечення

Вимоги до додаткового спеціального програмного забезпечення, яке необхідне для функціонування окремих складових частини комплексу наведені у таблиці 2.2.

Таблиця 2.2

Складова частина комплексу	Вимоги до спеціального програмного забезпечення
Програмні компоненти сервера синхронізації часу	Не висуваються
Програмні компоненти клієнта синхронізації часу	Не висуваються

З СКЛАД ТЕХНІЧНОГО ОБЛАДНАННЯ, ЩО ЗАСТОСОВУЄТЬСЯ У ПРОЦЕСІ СИНХРОНІЗАЦІЇ, ЙОГО ЗАГАЛЬНИЙ ОПИС

3.1 Структура комплексу засобів синхронізації часу

До складу комплексу входять такі технічні та програмні засоби:

- корпоративні NTP-сервери ЦЗО 212.90.164.90, 212.90.170.122, 81.17.128.133;
- сервер взаємодії ЦСК (NTP-сервер ЦСК);
- міжмережний екран та комутатор ПТК ЦСК;
- сервер синхронізації та моніторингу ЦСК із програмним комплексом сервера синхронізації часу “ІІТ Синхронізація часу-1. Сервер” та GPS-приймачем;
- PC та сервери ЦСК зі штатними програмними NTP-клієнтами ОС.

Структурна схема комплексу засобів синхронізації часу ЦСК наведена на рис. 3.1.

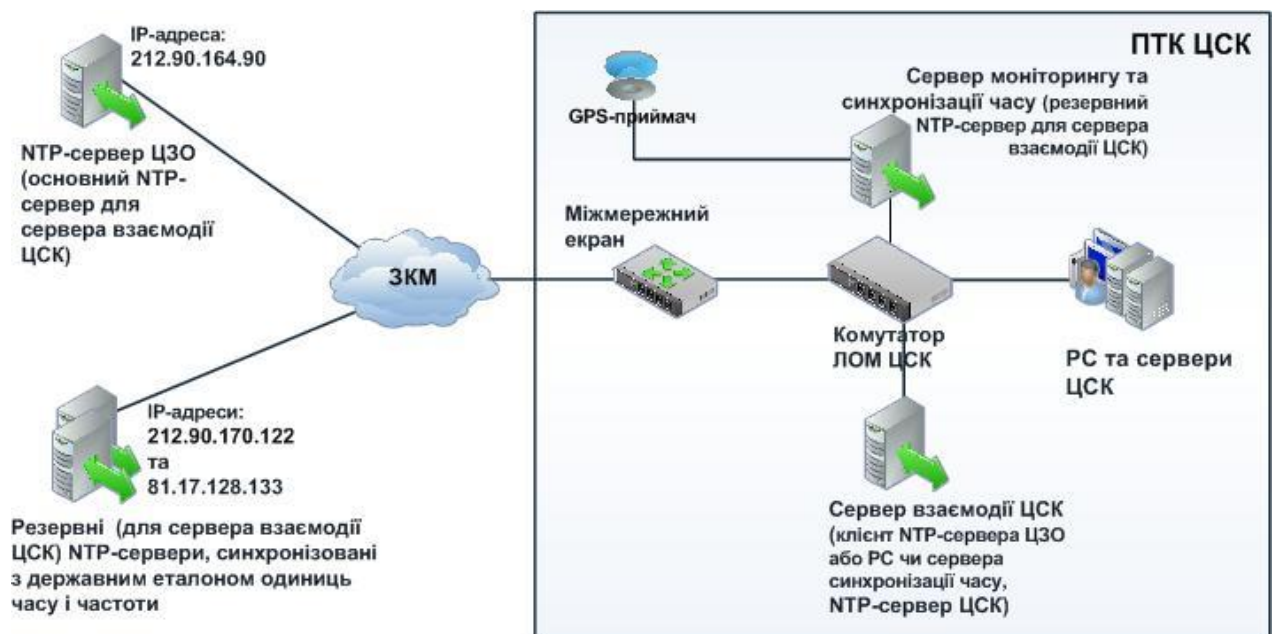


Рисунок 3.1- Структурна схема комплексу засобів синхронізації часу ЦСК.

3.2 Перелік технічних та програмних засобів синхронізації часу

Перелік технічних засобів ЦСК що входять до складу комплексу синхронізації часу наведений у табл. 3.1.

Перелік програмних засобів ЦСК що входять до складу комплексу синхронізації часу наведений у табл. 3.2.

Таблиця 3.1 - Технічні засоби ЦСК що входять до складу комплексу синхронізації часу.

Найменування	Характеристики
GPS-приймач	GPS-приймач EPS Agro-DM-1Hz
Міжмережний екран	Cisco ASA 5512
Комутатор	Cisco Catalyst 2960
Сервер взаємодії	HP Proliant DL360 G8
Сервер моніторингу та синхронізації часу	HP Proliant DL360 G8

Таблиця 3.2 - Програмні засоби ЦСК що входять до складу комплексу синхронізації часу.

Найменування	Характеристики
Сервер взаємодії	ОС: FreeBSD 9.2 Штатні NTP-клієнт та NTP-сервер ОС
Сервер моніторингу та синхронізації часу	ОС: FreeBSD 9.2 Штатні NTP-клієнт та NTP-сервер ОС
РС та сервери ЦСК	Штатні NTP-клієнти ОС

4 ПОРЯДОК СИНХРОНІЗАЦІЇ

4.1 Порядок синхронізації

NTP-клієнт сервера взаємодії ЦСК отримує значення часу від NTP-сервера ЦЗО або від та резервних NTP-серверів, синхронізованих з державним еталоном одиниць часу і частоти, із наступними параметрами:

- IP-адреса основного NTP-сервера ЦЗО - 212.90.164.90;
- IP-адреси резервних NTP-серверів, синхронізованих з державним еталоном одиниць часу і частоти (використовуються як основні тільки при аварійному відключенні основного NTP-сервера ЦЗО) - 212.90.170.122 та 81.17.128.133;
- номер UDP-порта - 123;
- інтервал опитування - 16 с;
- ознака перевірки контрольної суми UDP-пакетів - визначається на етапі налагодження в залежності від можливостей ОС сервера взаємодії.

Параметри NTP-клієнта сервера взаємодії ЦСК наведені у дод. 2.

Для можливості взаємодії із NTP-сервером ЦЗО або з резервними NTP-серверами, синхронізованими з державним еталоном одиниць часу і частоти, міжмережний екран ЦСК повинен мати правило, що дозволяє виконувати передачу UDP-пакетів з метою синхронізації часу. Приклад такого правила (для між мережних екранів типу Cisco ASA серії 5500) наведено нижче:

```
access-list OUTSIDE_INTERFACE extended permit udp host NTP_SERVER host  
INTERACTION_SERVER eq ntp,
```

де **OUTSIDE_INTERFACE** - назва інтерфейсу що підключений до зовнішньої телекомунікаційної мережі (далі - ЗТМ) передачі даних, **NTP_SERVER** - IP-адреса NTP-сервера ЦЗО, **INTERACTION_SERVER** - IP-адреса NTP-сервера ЦСК.

4.2 Методика синхронізації часу в штатних ситуаціях

Під час штатної роботи синхронізація часу здійснюється із підключенням до NTP-серверів ІТС ЦЗО (див. п. 4.1). Синхронізація часу здійснюється штатним програмним NTP-сервером ОС сервера взаємодії ЦСК що реалізований у вигляді демону (у ОС Linux - NTP daemon program) (див. п.3.4).

4.3 Методика синхронізації часу в аварійних ситуаціях

Якщо NTP-сервери ЦЗО (212.90.164.90 або 212.90.170.122, 81.17.128.133) стають недоступними, то синхронізація часу автоматично здійснюється із підключенням до резервного NTP-сервера для сервера взаємодії ЦСК.

Доступність NTP-серверів та пріоритетність для синхронізації визначається NTP-сервером ЦСК аналізується та встановлюється автоматично за алгоритмом роботи протоколу NTP та відповідно до конфігурації (дод. 1).

4.4 Операційний контроль

Контроль за станом синхронізації часу здійснюється шляхом аналізу відповідних журналів реєстрації подій - журналу подій NTP-сервера ЦСК, журналу подій РС (сервера) синхронізації часу, журналів подій РС та серверів ЦСК - NTP-клієнтів, а також шляхом візуального контролю значення часу на технічних засобах ПТК ЦСК.

Відповідальними особами щодо контролю за станом синхронізації часу у ЦСК є адміністратор безпеки та системний адміністратор.

ДОДАТОК 1. КОНФІГУРАЦІЯ NTP-СЕРВЕРА ЦЕНТРУ СЕРТИФІКАЦІЇ КЛЮЧІВ

Файл конфігурації ntp.conf штатного NTP-сервера ОС сервера взаємодії ЦСК для роботи в якості NTP-клієнта та NTP-сервера.

```
# NTP-сервер ЦЗО та резервні NTP-сервери
server 212.90.164.90 minpoll 4 maxpoll 7 iburst burst prefer
server 212.90.170.122 minpoll 4 maxpoll 7 iburst burst
server 81.17.128.133 minpoll 4 maxpoll 7 iburst burst

# NTP-сервер сервера синхронізації часу
server 192.168.100.40 minpoll 4 maxpoll 7 iburst burst

server 127.127.1.0
fudge 127.127.1.0 stratum 2

logfile /var/log/ntpd.log

# Файл, що містить інформацію про зміщення локального часу по відношенню до
# NTP-серверів
driftfile /var/db/ntp.drift

broadcastdelay 0.008

disable monitor

#restrict default nomodify noquery notrust

restrict default ignore

restrict localhost

restrict 127.0.0.1 mask 255.255.255.255

# Дозволи на синхронізацію часу з NTP-сервером ЦЗО та резервними NTP-серверами
restrict 212.90.164.90 mask 255.255.255.255
restrict 212.90.170.122 mask 255.255.255.255
restrict 81.17.128.133 mask 255.255.255.255

# Дозвіл на синхронізацію часу з NTP-сервером сервера синхронізації часу
restrict 192.168.100.40 mask 255.255.255.255

# Дозволи на синхронізацію часу для NTP-клієнтів ПТК (PC та серверів)
restrict 192.168.100.0 mask 255.255.255.0 nomodify notrap nopeer
```